

**IN THE UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF WISCONSIN**

JOHN DOE, <i>on behalf of himself and all others similarly situated</i> ,  Plaintiff,  v.  PROHEALTH CARE,  Defendant.	Case No. 23-cv-296  <b><u>JURY TRIAL DEMANDED</u></b>
----------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------

**CLASS ACTION COMPLAINT**

Plaintiff John Doe (“Plaintiff”)<sup>1</sup> brings this class action lawsuit in his individual capacity and on behalf of all others similarly situated against ProHealth Care (“ProHealth” or “Defendant”) and alleges, upon personal knowledge as to his own actions, his counsel’s investigation and upon information and good faith belief as to all other matters, as follows:

1. Plaintiff brings this case to address Defendant’s outrageous, illegal and widespread practice of disclosing Plaintiff’s and Class Members’ confidential personally identifiable information (“PII”) and protected health information (“PHI”) (collectively referred to as “Private Information”) to third parties, including Meta Platforms, Inc. d/b/a Meta (“Facebook”).

2. Information about a person’s physical and mental health is among the most confidential and sensitive information in our society and the mishandling of medical information

---

<sup>1</sup> In order to avoid compounding the injuries and damages which give rise to this putative class action lawsuit and given the highly sensitive nature of the non-public, confidential and highly sensitive personal health information of Plaintiff disclosed by Defendant without permission, Plaintiff will, contemporaneously with the filing of this Complaint, move this Honorable Court for permission to proceed anonymously. *See, e.g., Doe v. Bd. of Regents of Univ. of Wis. Sys.*, No. 19-cv-1348-pp, at \*3 (E.D. Wis. Sep. 8, 2020).

can have serious consequences, including discrimination in the workplace or denial of insurance coverage.

3. Simply put, if people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health consequences down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical providers is vitally necessary to maintain public trust in the healthcare system as a whole.

4. Recognizing these incontrovertible facts and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the United States Department of Health and Human Services ("HHS") has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information.

5. Under the HIPAA Privacy Rule, **no** health care provider may disclose a person's personally identifiable protected health information to a third party without express written authorization.

6. And, healthcare organizations regulated under HIPAA may use third-party tracking tools, such as Google Analytics or Meta Pixel, in a limited way, to perform analysis on data key to operations.

7. Covered entities such as ProHealth are simply ***not*** permitted, however, to use these tools in a way that may expose patients' protected health information to any third-party without express and informed consent:

Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or

any other violations of the HIPAA Rules. *For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.*<sup>2</sup>

8. Defendant owns, controls and maintains a website, [www.prohealthcare.org](http://www.prohealthcare.org) (the “Website”), which encourages patients to use for booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions and treatment options, signing up for events and classes, and more.

9. Plaintiff and other Class Members who visited and used Defendant’s Website understandably thought they were communicating only with their trusted healthcare provider.

10. Unbeknownst to Plaintiff and Class Members, however, Defendant had embedded the Facebook Tracking Pixel (the “Pixel” or “Facebook Pixel”) on its Website, which automatically transmits to Facebook every click, keystroke and intimate detail about their medical treatment.

11. Operating as designed and as implemented by Defendant, the Pixel allows the Private Information that Plaintiff and Class Members submit to Defendant to be unlawfully disclosed to Facebook alongside the individual’s unique and persistent Facebook ID (“FID”).<sup>3</sup>

12. A pixel is a piece of code that “tracks the people and [the] type of actions they take”<sup>4</sup> as they interact with a website, including how long a person spends on a particular web

---

<sup>2</sup> See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, available at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited March 2, 2023) (emphasis added).

<sup>3</sup> The Pixel forces the website user to share the user’s FID for easy tracking via the “cookie” Facebook stores every time someone accesses their Facebook account from the same web browser. “Cookies are small files of information that a web server generates and sends to a web browser”; “[c]ookies help inform websites about the user, enabling the websites to personalize the user experience.” See <https://www.cloudflare.com/learning/privacy/what-are-cookies/> (last visited March 2, 2023).

<sup>4</sup> FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited Feb. 17, 2023).

page, which buttons the person clicks, which pages they view, and the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), among other things.

13. The user's web browser executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner. The Facebook Pixel is thus customizable and programmable, meaning that the website owner controls which of its webpages contain the Pixel and which events are tracked and transmitted to Facebook.

14. By installing the Facebook Pixel on its Website, Defendant effectively planted a bug on Plaintiff's and Class Member's web browsers and compelled them to disclose their communications with Defendant to Facebook.

15. In addition to the Facebook Pixel, Defendant also installed and implemented Facebook's Conversions Application Programming Interface ("CAPI") on its Website servers.<sup>5</sup>

16. Unlike the Facebook Pixel, which coopts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers and then transmits the data to Facebook from the website owner's servers.<sup>6,7</sup>

---

<sup>5</sup> "CAPI works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." See <https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/> (last visited: January 25, 2023).

<sup>6</sup> <https://revealbot.com/blog/facebook-conversions-api/> (last visited: January 24, 2023).

<sup>7</sup> "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel.... This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." <https://developers.facebook.com/docs/marketing-api/conversions-api> (last visited: January 27, 2023).

17. Indeed, Facebook markets CAPI as a “better measure [of] ad performance and attribution across your customer’s full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results.”<sup>8</sup>

18. Because CAPI is located on the website owner’s servers and is not a bug planted onto the website user’s browser, it allows website owners like Defendant to circumvent any ad blockers or other denials of consent by the website user that would prevent the Pixel from sending website users’ Private Information to Facebook directly.

19. Defendant utilized the Pixel and CAPI data for marketing purposes in an effort to bolster its profits. That is, despite professing to “strive to continuously improve [the] community’s health and well-being by combining skill, compassion and innovation,”<sup>9</sup> Defendant put its own desires for profit over its patients’ privacy rights.

20. The Facebook Pixel and CAPI are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiff’s and Class Members’ Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendant.

21. The information that Defendant’s Tracking Pixel and CAPI sent to Facebook included the Private Information that Plaintiff and Class Members submitted to Defendant’s Website, including for example, the type of medical treatment sought, the individual’s particular health condition and the fact that the individual attempted to or did book a medical appointment.

---

<sup>8</sup> <https://www.facebook.com/business/help/2041148702652965?id=818859032317965> (last visited: January 28, 2023).

<sup>9</sup> <https://www.prohealthcare.org/about-us/> (last visited March 2, 2023).

22. Such information allows a third party (*e.g.*, Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers who geo-target Plaintiff's and Class Members' Facebook pages based on communications obtained via the Facebook Pixel and CAPI.

23. Facebook and any third-party purchasers of Plaintiff's and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia or HIV.

24. Healthcare patients simply do not anticipate that their trusted healthcare provider will send personal health information or confidential medical information collected via its webpages to a hidden third party – let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue – without the patients' consent.

25. Neither Plaintiff nor any other Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook.

26. Despite willfully and intentionally incorporating the Facebook Pixel and CAPI into its Website and servers, Defendant has never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook.

27. Plaintiff and Class Members were unaware that their Private Information was being surreptitiously transmitted to Facebook as they communicated with their healthcare provider via the Website, or stored on Defendant's servers to be later transmitted to Facebook so it could be used for targeted advertising and marketing purposes.

28. Defendant further made expressed and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with Defendant.

29. Defendant owed common law, statutory and regulatory duties to keep Plaintiff's and Class Members' communications and medical information safe, secure, and confidential.

30. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and to safeguard that information from unauthorized disclosure.

31. Defendant breached its statutory and common law obligations to Plaintiff and Class Member by, *inter alia*,: (i) failing to adequately review its marketing programs and web based technology to ensure the hospital Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through Facebook Pixels; (v) failing to warn Plaintiff and Class Members and (vi) otherwise failing to design, and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

32. As a result of Defendant's conduct, Plaintiff and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Pixel, (iii) loss of benefit of the bargain, (iv) diminution of value of the Private Information, (v) statutory damages and (v) the continued and ongoing risk to their Private Information.

33. Plaintiff seeks to remedy these harms and bring causes of action for (1) Invasion of Privacy, (2) Unjust Enrichment; (3) Breach of Confidence; (4) Violation of Wisconsin's Confidentiality of Patient Health Care Records Act (Wis. Stat. § 146.81 *et seq.*); (5) violations of the Electronics Communication Privacy Act ("ECPA") 18 U.S.C. § 2511(1) -unauthorized

interception, use, and disclosure; (6) violations of ECPA, 18 U.S.C. § 2511(3)(a) -unauthorized interception, use, and disclosure; (7) violations of Title II of the ECPA, 18 U.S.C. § 2702, *et seq.*, - Stored Communications Act; and (8) Violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030, *et seq.*).

## **I. PARTIES**

34. Plaintiff John Doe is a natural person and citizen of Wisconsin, residing in Hubertus, Wisconsin, where he intends to remain.

35. Defendant ProHealth is a registered non-profit entity with its headquarters and principal place of business at N17W24100 Riverwood Drive in Waukesha, Wisconsin.

36. Defendant ProHealth is the largest health care system between Milwaukee and Madison, employing 6,000 employees and nearly 1,000 doctors and other health professionals treating more than 400,000 patients a year.

37. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d & 45 C.F.R. Part 160-45 C.F.R. Part 162, & 45 C.F.R. Part 164 (“HIPAA”).

## **II. JURISDICTION & VENUE**

38. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because it arises under the laws of the United States and under 28 U.S.C. § 1332(d) because this is a class action lawsuit wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, is a citizen of a state different from Defendant.



39. This Court has federal question jurisdiction under 29 U.S.C. § 1331 because this Complaint alleges questions of federal laws under the ECPA (28 U.S.C. § 2511, *et seq.*, and 28 U.S.C. § 2702) and the CFAA (18 U.S.C. § 1030, *et seq.*).

40. This Court has personal jurisdiction over Defendant because its principal place of business is in this judicial district and a substantial portion of the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this judicial district.

41. Venue is proper under 18 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in this judicial district.

### **III. COMMON FACTUAL ALLEGATIONS**

#### ***A. Background: Underlying Technology Employed by Defendant for the Purpose of Disclosing Plaintiff and Class Members' Private Information to Facebook.***

42. Defendant ProHealth owns and operates more than 26 healthcare facilities including 4 hospitals, 3 emergency departments, 11 urgent care clinics, 3 cancer centers, 15 medical clinics (known as ProHealth Medical Group), 4 pharmacies and 16 rehabilitation centers.<sup>10</sup>

43. As the owner and operator of ProHealth Waukesha Memorial Hospital ("WMH") and the ProHealth Medical Group Clinic at Sussex ("MG Clinic"), among other medical centers and entities, Defendant ProHealth offers a wide range of services, from primary and urgent care to cancer treatment, heart and vascular, orthopedics, hospice care, occupational health and senior living.

44. Defendant purposely installed the Pixel and CAPI tools on its Website and programmed the Website to surreptitiously share its patients' private and protected

---

<sup>10</sup> See <https://www.prohealthcare.org/about-us/> (last visited March 2, 2023).

communications with Facebook, including communications that contain Plaintiff's and Class Members' PHI and PII.

45. On numerous occasions, with the most recent being in December 2022, Plaintiff Doe accessed Defendant's Website on his mobile device and computer and used the Website to look for providers at WMH and MG Clinic to arrange care and treatment to make appointments and to pay bills.

46. Plaintiff has used and continues to use the same devices to maintain and to access an active Facebook account throughout the relevant period in this case.

47. Further to the systematic process described herein, ProHealth assisted Facebook with intercepting Plaintiff's communications, including those that contained personally identifiable information, protected health information and related confidential information.

48. Defendant assisted these interceptions without Plaintiff Doe's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff Doe personally identifiable information and protected health information.

49. Defendant uses the Website to connect Plaintiff and Class Members to Defendant's digital healthcare platforms with the goal of increasing profitability.

50. In order to understand Defendant's unlawful data sharing practices, it is important to first understand basic web design and tracking tools.

**1. Facebook's Business Tools & the Pixel**

51. Facebook operates the world's largest social media company and generated \$117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.<sup>11</sup>

52. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendant, to utilize its "Business Tools" to gather, identify, target and market products and services to individuals.

53. Facebook's Business Tools, including the Pixel and CAPI, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

54. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.<sup>12</sup> Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."<sup>13</sup>

---

<sup>11</sup> FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx> (last visited Nov. 14, 2022).

<sup>12</sup> FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, <https://www.facebook.com/business/help/402791146561655?id=1205376682832142>. (last visited Nov. 14, 2022); *see* FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, <https://developers.facebook.com/docs/facebook-pixel/advanced/>; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>; FACEBOOK, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/> (last visited Nov. 14, 2022).

<sup>13</sup> FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, <https://www.facebook.com/business/help/964258670337005?id=1205376682832142>; *see also* FACEBOOK, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/>. (last visited Nov. 14, 2022).

55. One such Business Tool is the Pixel which “tracks the people and type of actions they take.”<sup>14</sup> When a user accesses a webpage that is hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook’s servers—traveling from the user’s browser to Facebook’s server.

56. Notably, this transmission only occurs on webpages that contain the Pixel. Thus, Plaintiff’s and Class Member’s Private Information would not have been disclosed to Facebook via the Pixel but for Defendant’s decisions to install the Pixel on its Website.

57. Similarly, Plaintiff’s and Class Member’s Private Information would not have been disclosed to Facebook via CAPI but for Defendant’s decision to install and implement that tool.

58. By installing and implementing both tools, Defendant caused Plaintiff’s and Class Members’ communications to be intercepted and transmitted to Facebook via the Pixel, and it caused a second improper disclosure of that information via CAPI.

59. As explained below, these unlawful transmissions are initiated by Defendant’s source code concurrent with communications made via the Website.

**2. *Defendant’s method of transmitting Plaintiff’s and Class Members’ Private Information via the Tracking Pixel and/or CAPI i.e., the interplay between HTTP Requests and Responses, Source Code & the Pixel***

60. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each “client device” (such as computer, tablet, or smart phone) accessed web content through a web browser (e.g., Google’s Chrome browser, Mozilla’s Firefox browser, Apple’s Safari browser, and Microsoft’s Edge browser).

---

<sup>14</sup> FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting>.

61. Every website is hosted by a computer “server” that holds the website’s contents and through which the entity in charge of the website exchanges communications with Internet users’ client devices via their web browsers.

62. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **HTTP Request**: an electronic communication sent from the client device’s browser to the website’s server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are “third-party cookies” which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response**: an electronic communication that is sent as a reply to the client device’s web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.<sup>15</sup>

---

<sup>15</sup> One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

63. A patient's HTTP Request essentially asks the Defendant's Website to retrieve certain information (such as a physician's "Book an Appointment" page), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Website).

64. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

65. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Defendant's Pixel is source code that does just that. The Pixel acts much like a traditional wiretap.

66. When patients visit Defendant's website via an HTTP Request to ProHealth's server, Defendant's server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendant's Pixel.

67. Thus, Defendant is in essence handing patients a tapped phone, and once the Webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third-parties, including Facebook and Google.

68. Third parties, like Facebook, place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each

intercepted communication to ensure the third-party can uniquely identify the patient associated with the Personal Information intercepted.

69. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on gathering Personal Information, like Facebook, implement workarounds that cannot be evaded by savvy users.

70. Facebook's workaround, for example, is called CAPI. CAPI is an effective workaround because it does not intercept data communicated from the user's browser. Instead, CAPI "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]."

71. Thus, the communications between patients and Defendant, which are necessary to use Defendant's Website, are actually received by Defendant and stored on its server before CAPI collects and sends the Private Information contained in those communications directly from Defendant to Facebook.

72. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

73. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like CAPI without access to the host server, companies like Facebook instruct Defendant to "[u]se the CAPI in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."<sup>16</sup> Thus, it is reasonable to infer that Facebook's

---

<sup>16</sup> See <https://www.facebook.com/business/help/308855623839366?id=818859032317965> (last visited Jan. 23, 2023).

customers who implement the Facebook Pixel in accordance with Facebook's documentation will also implement the CAPI workaround.

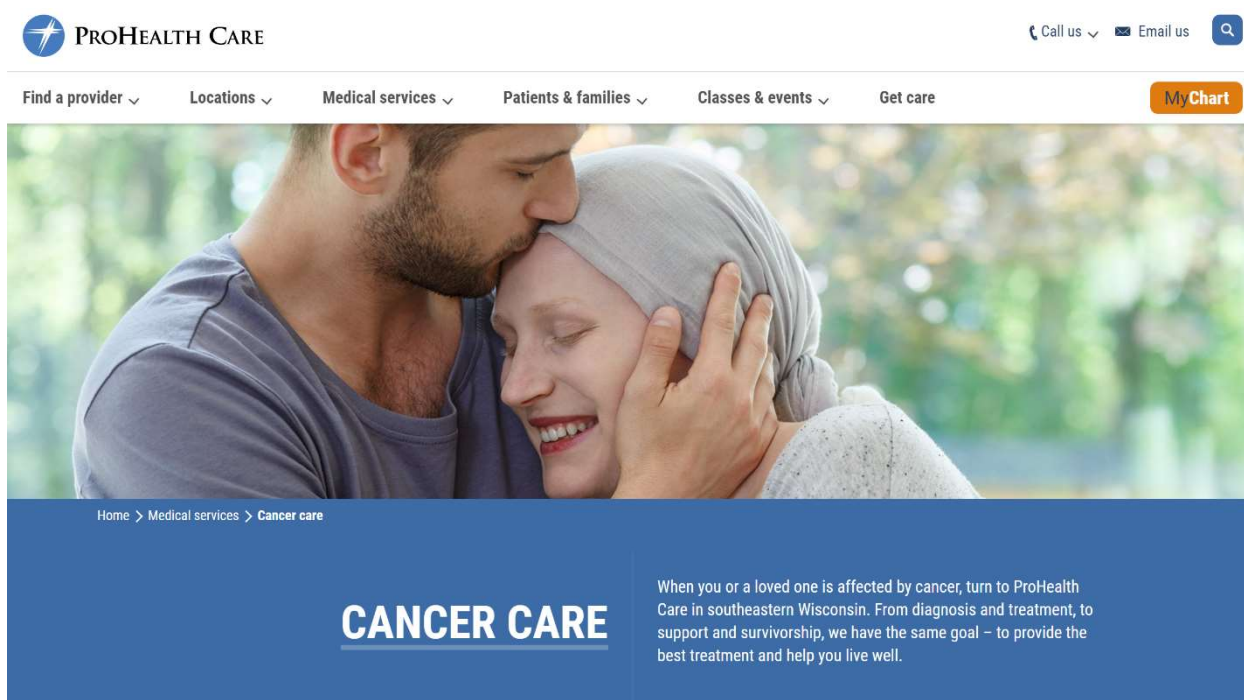
74. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content relating to the user's communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner (i.e., to bolster profits).

75. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

76. In this case, Defendant employed the Tracking Pixel and CAPI to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to Facebook.

77. For example, when a patient visits [www.prohealthcare.org/medical-services/](http://www.prohealthcare.org/medical-services/) and selects "Cancer Care," the patient's browser automatically sends an HTTP Request to Defendant's web server. The Defendant's web server automatically returns an HTTP Response, which loads the Markup for that particular webpage as depicted below.





*Figure 1. Image taken from <https://www.prohealthcare.org/medical-services/cancer-care/>*

78. The patient visiting this particular web page only sees the Markup, not the Defendant's Source Code or underlying HTTP Requests and Responses.

79. In addition to controlling a website's Markup, Source Code executes a host of other programmatic instructions and can command a website visitor's browser to send data transmissions to third parties via pixels or web bugs,<sup>17</sup> effectively open a spying window through which the webpage can funnel the visitor's data, actions, and communications to third parties.

80. Looking to the previous example, Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) and send those communications to Facebook.

<sup>17</sup> These pixels or web bugs are tiny image files that are invisible to website users. They are purposefully designed in this manner, or camouflaged, so that users remain unaware of them.

81. This occurs because the Pixel embedded in Defendant's Source Code is programmed to automatically track and transmit patient's communications, and this occurs contemporaneously, invisibly, and without the patient's knowledge.

82. Thus, without its patients' consent, Defendant has effectively used its source code to commandeer patients' computing devices, thereby re-directing their Private Information to third parties.

83. The information that Defendant's Pixel sends to Facebook may include, amongst other things, patients' PII, PHI, and other confidential information.

84. Consequently, when Plaintiff and Class Members visit Defendant's website and communicate their Private Information, it is transmitted to Facebook, including, but not limited to, appointment type and date, physician selected, specific button/menu selections, content typed into free text boxes, demographic information, email addresses, phone numbers, and emergency contact information.

***B. Defendant's Pixel and/or CAPI Tracking Practices caused Plaintiff's and Class Members' PII and PHI to be sent to Facebook.***

85. Defendant utilizes Facebook's Business Tools and intentionally installed the Pixel and CAPI on its Website to secretly track patients by recording their activity and experiences in violation of its common law, contractual, statutory, and regulatory duties and obligations.<sup>18</sup>

86. Defendant's Webpages contain a unique identifier which indicates that the Pixel is being used on a particular webpage, identified as 374308662930239 on [www.prohealthcare.org](http://www.prohealthcare.org).

---

<sup>18</sup> *Id.*

87. The Pixel allows Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs.<sup>19</sup> However, Defendant's Website do not rely on the Pixel in order to function.

88. While seeking and using Defendant's services as a medical provider, Plaintiff and Class Members communicated their Private Information to Defendant via its Website.

89. Defendant did not disclose to Plaintiff and Class Members that their Private Information would be shared with Facebook as it was communicated to Defendant.

90. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to Facebook, nor did they intend for Facebook to be a party to their communications with Defendant.

91. Defendant's Pixel and CAPI sent non-public Private Information to Facebook, including but not limited to Plaintiff's and Class Members': (1) status as medical patients; (2) health conditions; (3) sought treatment or therapies; (4) appointment requests and appointment booking information; (5) registration or enrollment in medical classes (such as breastfeeding courses); (6) locations or facilities where treatment is sought; (7) which webpages were viewed and (8) phrases and search queries conducted via the general search bar.

92. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside the Plaintiff's and Class Members' Facebook ID (c\_user cookie or "FID"), thereby allowing individual patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts.<sup>20</sup>

---

<sup>19</sup> *Id.*

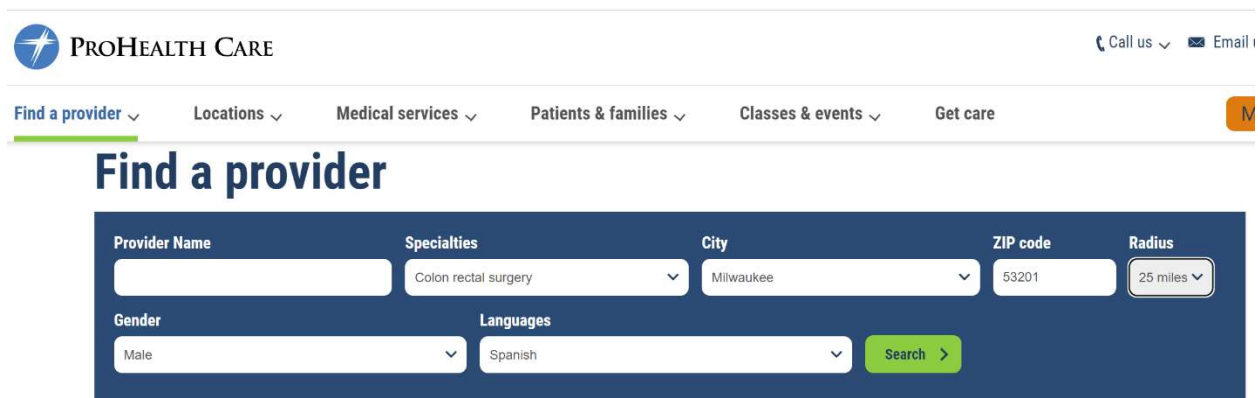
<sup>20</sup> Defendant's Website track and transmit data via first-party and third-party cookies. The c\_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

93. A user’s FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user’s Facebook Profile ID uniquely identifies an individual’s Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user’s corresponding Facebook profile.

94. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented technology (i.e., the Facebook Pixel) that surreptitiously tracked, recorded, and disclosed Plaintiff’s and other online patients ’confidential communications and Private Information; (2) disclosed patients ’protected information to Facebook—an unauthorized third-party; and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

***C. Defendant’s Pixel Disseminates Patient Information via [www.ProHealthCare.org](http://www.ProHealthCare.org)***

95. An example illustrates the point. If a patient uses [www.prohealthcare.org](http://www.prohealthcare.org) to look for a doctor, they may select the “Find a Provider” tab, which takes them to the “Find a Provider” page.

The image shows a screenshot of the ProHealth Care website's "Find a provider" page. At the top, the ProHealth Care logo is on the left, and "Call us" and "Email" links are on the right. Below the header is a navigation bar with tabs: "Find a provider" (highlighted), "Locations", "Medical services", "Patients & families", "Classes & events", and "Get care". The main heading "Find a provider" is in large blue text. Below it is a search form with a dark blue background. The form contains several input fields: "Provider Name" (text input), "Specialties" (dropdown menu with "Colon rectal surgery" selected), "City" (dropdown menu with "Milwaukee" selected), "ZIP code" (text input with "53201"), "Radius" (dropdown menu with "25 miles"), "Gender" (dropdown menu with "Male" selected), and "Languages" (dropdown menu with "Spanish" selected). A green "Search" button with a right arrow is at the bottom right of the form.

***Figure 2. Defendant directs patients to its “Find a Provider” webpage with embedded Pixels – which are invisible to the regular user.***

96. On this page Defendant asks to user to narrow their search results by “Provider Name,” “Specialties,” “City,” “ZIP code” (with an option to choose a certain radius), “Gender,” “Languages,” or “accepting new patients.”

97. If a user selects filters or enters keywords into the search bar on the “Find a Provider” webpage, the filters and search terms are transmitted via the Facebook Pixel. Similarly, if a patient uses the Website’s general search bar or chat, the terms and phrases the patient types are transmitted to Facebook, even if they contain a patient’s treatment, procedures, medical conditions, and related queries. This information is automatically sent from the patient’s device to Facebook, and it reveals the patients FID (c\_user field) along with each search filter the patient selected.

98. Without alerting the user, Defendant’s Pixel sends each and every communication the user made to the Defendant via the Webpage to Facebook, and the image below confirms that the communications Defendant sends to Facebook contain the user’s Private Information.

The image shows a network request header for a GET request to www.facebook.com. The path contains search parameters: city=3DMilwaukee, gender=3Dmale, zipCode=3053201, radius=3025. The cookie field shows c\_user=54. The referer is https://www.prohealthcare.org/.

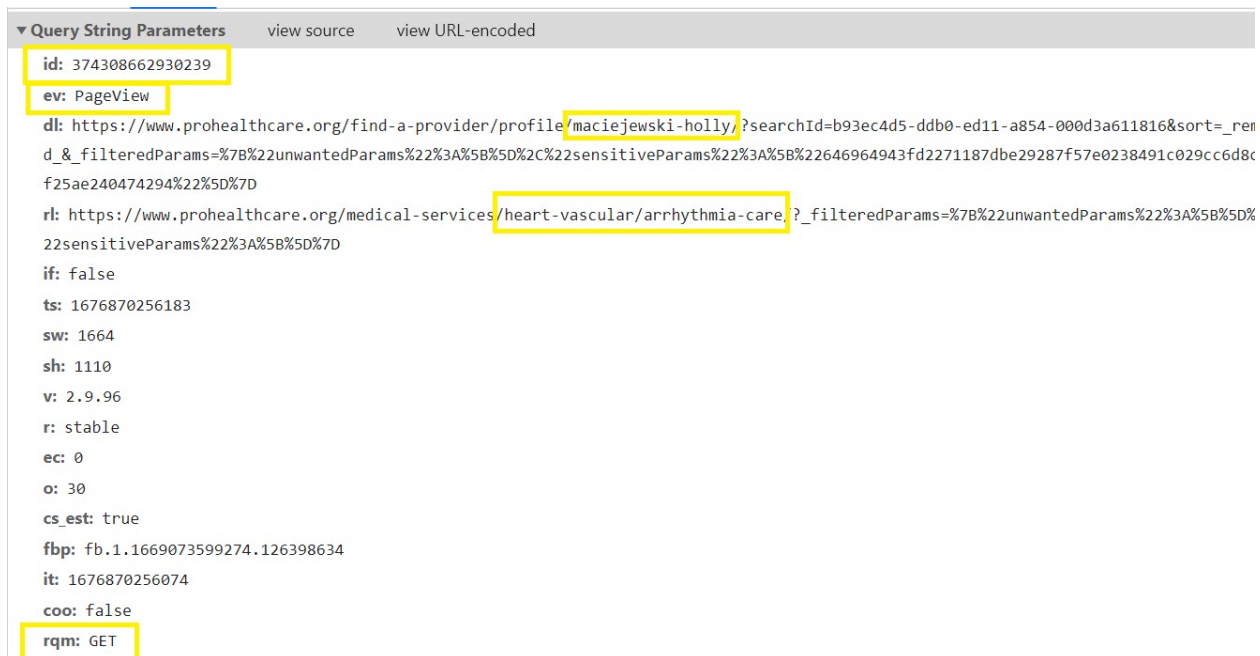
```
▼ Request Headers
:authority: www.facebook.com
:method: GET
:path: /tr/?id=374308662930239&ev=PageView&dl=https%3A%2F%2Fwww.prohealthcare.org%2Ffind-a-provider%2F%3FtermId%3De614bf42-1792-e911-a820-000d3a619f08%26city%3DMilwaukee%26gender%3Dmale%26zipCode%3053201%26radius%3025%26page%3D1&rl=https%3A%2F%2Fwww.prohealthcare.org%2Ffind-a-provider%2F&if=false&ts=1676869192597&sw=1664&sh=1110&v=2.9.96&r=stable&ec=0&o=30&cs_est=true&fbp=fb.1.1669073599274.126398634&it=1676869191879&coo=false&rqm=GET
:scheme: https
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9,ru;q=0.8
cookie: c_user=54 datr=QtI1Y1lVd2UW0uuBmn2Mb8vC; dpr=1.5; xs=188%3AWgt7jCKaF4RNPg%3A2%3A1597289338%3A-1%3A3037%3A%3AAcW9C6F5gz4j_AkqnHx21jttjHX5rs6WsmTvvrrps39w; usida=eyJ2ZXI0JEsImkIjoiQXJxOHVuaZFMdWJtZmU1LCJ0aw11IjoxNjc2NjY5NzQ0fQ%3D%3D; fr=09xocanw5tE9ZU6hi.AwVTjnfONjDeSzfQiny3ILZvVow.Bj7mtx.-f.AAA.0.0.Bj7_Mv.AWVGyJ4cDKw
referer: https://www.prohealthcare.org/
```

**Figure 3. Defendant’s transmission to Facebook of patient’s search parameters showing search terms (“male” provider in “Milwaukee” within a 25 mile radius of the 53201 zip code) and the patient’s c\_user information from Defendant’s “Find a Provider” webpage.**

99. After taking any of these actions on the Find a Provider page, patients are subsequently directed to the “Provider Search Results” page, and their selections or search parameters are automatically transmitted by the Pixel to Facebook.

100. For example, searching for an arrhythmia specialist brings the user to a page listing Defendant’s heart and vascular specialists, including Dr. Holly Maciejewski.

101. Once a patient chooses a doctor, all of the information that patient has submitted is automatically sent directly to Facebook. The information transmitted to Facebook includes: (i) the patient’s unique and persistent Facebook ID (c\_user ID), (ii) the fact that the patient clicked on a specific provider’s profile page (Dr. Maciejewski in the example above and below), (iii) the patient’s search parameters (demonstrating they specifically searched for a female or male doctor and their specialty), and (iv) the patient’s location filter.



**Figure 4. An HTTP single communication session sent from the device to Facebook that reveals the user’s search parameters and results.**

102. The first line of highlighted text, “id: 374308662930239,” refers to the Defendant’s Pixel ID for this particular Webpage and confirms that the Defendant has downloaded the Pixel into its Source Code on this particular Webpage.

103. The second line of text, “ev: PageView,” identifies and categorizes which actions the user took on the Webpage (“ev:” is an abbreviation for event, and “PageView” is the type of event). Thus, this identifies the user as having viewed the particular Webpage.

104. The remaining lines of text identify: (1) the user as a patient seeking medical care from Defendant via www.prohealthcare.org; (2) who is in the process of looking at a specific provider; (3) the provider specializes in heart and vascular diseases; and (4) specifically in arrhythmia care.


105. Finally, the last line of highlighted text (“GET”), demonstrates that Defendant’s Pixel sent the user’s communications, and the Private Information contained therein, alongside the user’s Facebook ID (c\_user ID). This is further evidenced by the image below, which was collected during the same browsing session as the previous image.<sup>21</sup>

```
▼ Request Headers
:authority: www.facebook.com
:method: GET
:path: /tr/?id=374308662930239&ev=PageView&f1=https%3A%2F%2Fwww.prohealthcare.org%2Ffind-a-provider%2Fprofile%2Fmaciejewski-holly%2F%3FsearchId%3De0b211f-ab7c-ed11-a852-000d3a611816%26sort%3D_removed%26_filteredParams%3D%2578%2522unwantedParams%2522%253A%2558%255D%252C%2522sensitiveParams%2522%253A%2558%2522%252646964943fd2271187dbe29287f5e0238491c029cc6d8ce76f25ae240474294%2522%255D%257D&r1=https%3A%2F%2Fwww.prohealthcare.org%2Fmedical-services%2Fheart-vascular%2Farrhythmia-care%2F%3F_filteredParams%3D%2578%2522unwantedParams%2522%253A%2558%255D%252C%2522sensitiveParams%2522%253A%2558%255D%257D&if=false&ts=1671131069242&sw=1664&sh=1110&v=2.9.90&r=stable&ec=0&o=30&fbp=fb.1.1669073599274.126398634&it=1671131069171&coo=false&rqm=GET&dt=nlgz8qh9f9yh56o3f0nf5tqwaij83mw2
:scheme: https
:accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
:accept-encoding: gzip, deflate, br
:accept-language: en-US,en;q=0.9,ru;q=0.8
:cookie: c_user=54; datr=QtI1Y1lVd2UwOuuBmn2Mb8vC; m_page_voice=540643061; dpr=1.5; xs=188%3AWgt7jCKaF4RNPg%3A2%3A1597289338%3A-1%3A3037%3A3AAcWneeGZPyz4TIC_JOMqcjYunsVAXqocQokBmXDQXUQ; fr=0KFhRAKkpanAqenxr.AWU_E05b-wxhu3p2N0Idn1K6e-I.Bjm2xa.-f.AAA.0.0.Bjm2xa.AWUYWlMb-oY
:referrer: https://www.prohealthcare.org/
```

**Figure 5. An HTTP single communication session sent from the device to Facebook that reveals the search parameters and the patient’s FID (c\_user field).**

<sup>21</sup> The user’s Facebook ID is represented as the c\_user ID highlight in the image above, and Plaintiff has redacted the corresponding string of numbers to preserve the user’s anonymity.





VIEW OR CLOSE ALERT

Find a provider

Locations

Medical services

Patients & families

Classes & events

Home

Find a provider

Find a provider profile

Facebook Pixel Helper

Learn More

One pixel found on www.prohealthcare.org

Facebook Pixel

Pixel ID: 374308662830239 click to copy

Button Click Automatically Detected

PageView

Microdata Automatically Detected

Troubleshoot F

View Anal

HOLLY MACIEJEWSKI,

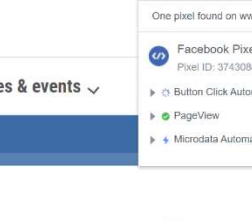
APNP

Electrophysiology

SCHEDULE AN APPOINTMENT

262-928-8800

Insurance accepted



**Request Headers**

:authority: www.facebook.com  
:method: GET  
  
:path: /tr/?id=374308662930239&ev=SubscribedButtonClick&l=https%3A%2F%2Fwww.prohealthcare.org%2Ffind-a-provider%2Fprofile%2Fmaciejewski-holly-2f%3FsearchId%3D0e0b211f-ab7c-ed11-a852-000d3a611816%26sort%3D3&r!l=https%3A%2F%2Fwww.prohealthcare.org%2Fmedical-services%2Fheart-vascular%2Farrhythmia-care%2Fif=false&ts=1671131132352&c&d%5BbuttonFeatures%5D=%7B%22classList%22%3A%22button%22callBtn%22%2C%22destination%22%3A%22tel%3A%2B1262-928-8800%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22262-928-8800%22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%22%3Anull%2C%22name%22%3A%22%22%27%0&c&d%5BbuttonText%5D=0-0-0&c&d%5BformFeatures%5D=%5B%5D&c&d%5BpageFeatures%5D=%7B%22title%22%3A%22Scn%2FHolly%20Maciejewski%2C%20APNP%20%27%20Cardiology%20%27%20Waukesha%2C%20WI%22%20%27%20ProHealth%20Care%5Cn%22%27%20&c&d%5Bparameters%5D=%5B%5D&s=w=1664&sh=1110&v=2.9.90&r=stable&ec=&eo=30&fbp=fb.1.1669073599274.126398634&it=1671131069171&coo=false&es=automatic&tm=3&rqm=GET&t=wtgbeenjcxec9c21ak6bl92anq1086c  
  
:scheme: https  
  
accept: image/avif,image/webp,image/apng,image/svg+xml,image/\*,\*/\*;q=0.8  
accept-encoding: gzip, deflate, br  
accept-language: en-US,en;q=0.9,ru;q=0.8  
  
cookie: c\_user=541; datr=QtI1Y1VldUwOuuBmn2Mbvc8; m\_page\_voice=540643061; dpr=1.5; xs=188%3Awgt7jKcAFARNPg%3A2%3A1597289338%3A-1%3A3037%3A3AACwneeGPyZ4TIC\_QJMQjYjunsyVAxQocQkBMXQXuQ; fr=0&FhRAKKpanAqenxr.AwU\_E05b-wxhu3p2N0Idn1K6E-I.Bjm2xa.-f.AAA.0.0.Bjm2xa.AwUWM1Mb-oY  
  
referer: https://www.prohealthcare.org/  
sec-ch-ua: "Google Chrome";v="107", "Chromium";v="107", "Not=A?Brand";v="24"

Case 2:23-cv-00296-BHL Filed 03/03/23 Page 24 of 69 Document 1



109. The examples below demonstrate that, if a user searches for “brain cancer” or clicks on “Support Groups” for “Traumatic Brain Injury,” Defendant’s Pixel shares that information with Facebook as well:

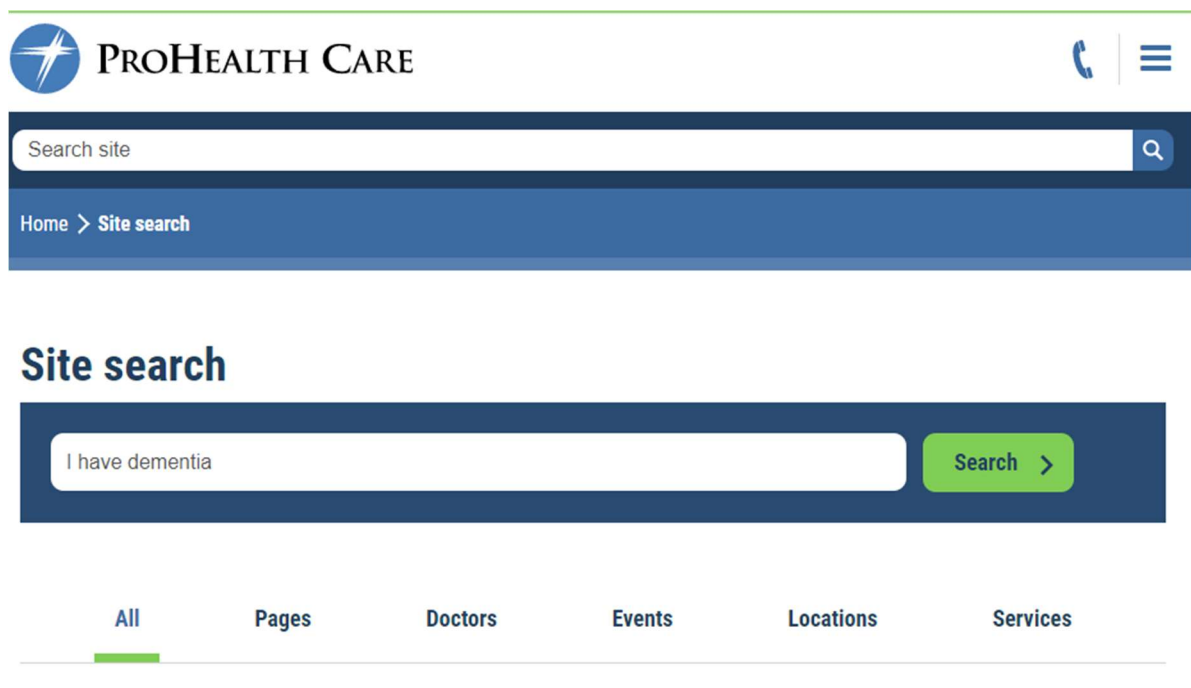
```

▼ Request Headers
:authority: www.facebook.com
:method: GET
:path: /tr/?id=374308662930239;ev=Microdata;dl=https%3A%2F%2Fwww.prohealthcare.org%2Fclasses-events%2Fsearch-results-detail%2F%3FeventId%3D51d6d3ea-a333-ed11-a851-000d3a611816&rl=https%3A%2F%2Fwww.prohealthcare.org%2Fclasses-events%2Fevent-results%2F%3FtermId%3Da-f70122c-dcaf-ea11-a82d-000d3a611816&if=false&ts=1676867474717&cd[DataLayer]=%5B%5D&cd[Meta]=%7B%22title%22%3A%22%5Cn%5C%20Traumatic%20Brain%20Injury%20Support%20Group%5Cn%22%7D&cd[OpenGraph]=%7B%7D&cd[Schema.org]=%5B%5D&cd[JSON-LD]=%5B%5D&sw=1664&sh=1110&v=2.9.96&r=stable&ec=1&o=30&fbp=fb.1.1669073599274.126398634&it=1676867472930&coo=false&es=automatic&tm=3&rqm=GET
:scheme: https
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9,ru;q=0.8
cookie: c_user=54 datr=Qt1IY1lVd2UW0uuBmn2Mb8vC; dpr=1.5; xs=188%3Awgt7jCKaF4RNPg%3A2%3A1597289338%3A-1%3A3037%3A3AAcW9CF5gz4j_AqknHx21j1tjHX5r6wsMtvrrps39w; usida=eyJ2ZXIiOiEiImklrjoiQXQxOHVuaZfmdwJtZmUilCj0aW1lIjoxNjc2MjY5NzQ0fQ%3D%3D; fr=09xocanw5tE9ZU6hi.AWtJnfnONjdesZfQIny3ILZVvow.Bj7mtx.-f.AAA.0.0.Bj7_Mv.AWVGJY4cDKW
referer: https://www.prohealthcare.org/

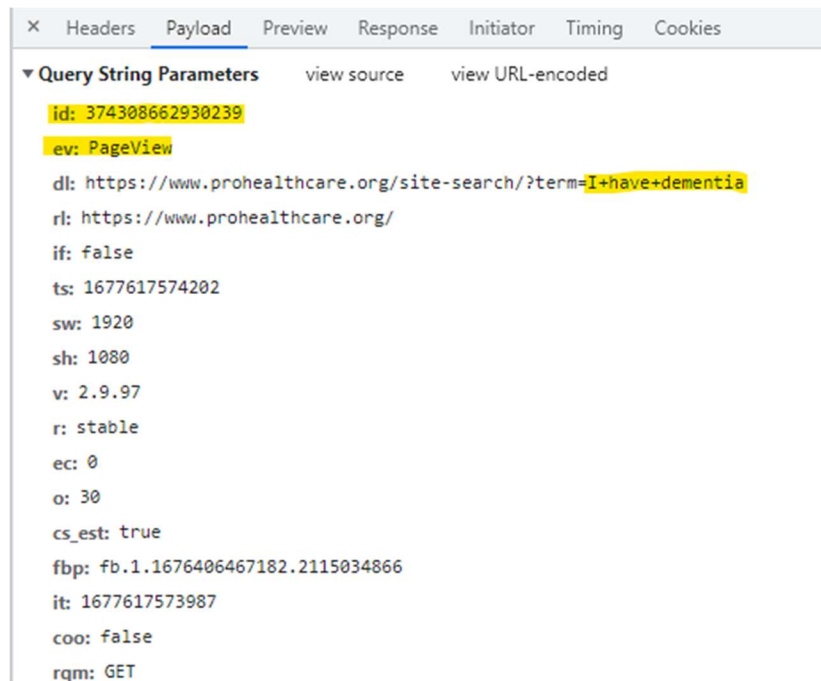
```

110. To make matters worse, the text and phrases that patients type into the search bar are also sent to Facebook.

111. The images below demonstrate that when a user types the phrase “I have dementia” into the general search bar, that exact phrase is sent to Facebook alongside the user’s Facebook ID, thereby allowing the phrase and medical condition contained therein to be attributed and associated with their individual Facebook account.



The screenshot displays the ProHealth Care website's search interface. At the top, the ProHealth Care logo is on the left, and a phone icon and a hamburger menu icon are on the right. Below the logo is a search bar with the placeholder text "Search site" and a magnifying glass icon. Below the search bar is a blue navigation bar with the text "Home > Site search". Below the navigation bar is the "Site search" section. It features a large search bar with the text "I have dementia" and a green "Search >" button. Below the search bar are six filter tabs: "All", "Pages", "Doctors", "Events", "Locations", and "Services". The "All" tab is currently selected, indicated by a green underline.



***Figures 10 and 11. Example of exact text and phrases being shared with Facebook.***

112. Each time Defendant sends this activity data, it also discloses a patient's personally identifiable information alongside the contents of their communications.

113. A user who accesses Defendant's website while logged into Facebook will transmit the c\_user cookie to Facebook, which contains that user's unencrypted Facebook ID.

114. When accessing prohealthcare.org, for example, Facebook receives six cookies:

Request Cookies <input type="checkbox"/> show filtered out request cookies		
Name	Value	Domain
c_user	540...	.facebook.com
datr	Qt11...	.facebook.com
m_page_voice	540...	.facebook.com
dpr	1.5	.facebook.com
xs	188...	.facebook.com
fr	OKF...	.facebook.com

***Figure 12.***

115. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies<sup>22</sup>:

fr	00Zp...	.facebook.com
wd	1156...	.facebook.com
sb	qqAz...	.facebook.com
datr	Malz...	.facebook.com

**Figure 13.**

116. The fr cookie contains, at least, an encrypted Facebook ID and browser identifier.<sup>23</sup> Facebook, at a minimum, uses the fr cookie to identify users.<sup>24</sup>

117. At each stage, Defendant also utilized the \_fbp cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user:<sup>25</sup>

_fbp	fb.1.1669073599274.126398634	.prohealthcare.org
------	------------------------------	--------------------

118. The fr cookie expires after 90 days unless the visitor's browser logs back into Facebook.<sup>26</sup>

119. If that happens, the time resets, and another 90 days begins to accrue.<sup>27</sup>

120. The \_fbp cookie expires after 90 days unless the visitor's browser accesses the same website.<sup>28</sup>

---

<sup>22</sup> The screenshot below serves as example and demonstrates the types of data transmitted during an HTTP single communication session. Not pictured here and in the preceding image is the \_fbp cookie, which is transmitted as a first-party cookie.

<sup>23</sup> Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit* (Sept. 21, 2012), p. 33, [http://www.europe-v-facebook.org/ODPC\\_Review.pdf](http://www.europe-v-facebook.org/ODPC_Review.pdf) (last visited Jan. 18, 2023).

<sup>24</sup> *Cookies & other storage technologies*, FACEBOOK.COM, <https://www.facebook.com/policy/cookies/> (last visited Jan. 18, 2023).

<sup>25</sup> *Id.*

<sup>26</sup> *Id.*

<sup>27</sup> Confirmable through developer tools.

<sup>28</sup> *Cookies & other storage technologies*, FACEBOOK.COM, <https://www.facebook.com/policy/cookies/> (last visited Jan. 18, 2023).

121. If that happens, the time resets, and another 90 days begins to accrue.<sup>29</sup>

122. The Facebook Tracking Pixel uses both first- and third-party cookies. A first-party cookie is “created by the website the user is visiting”—i.e., Defendant.<sup>30</sup>

123. A third-party cookie is “created by a website with a domain name other than the one the user is currently visiting”—i.e., Facebook.<sup>31</sup>

124. The `_fbp` cookie is always transmitted as a first-party cookie. A duplicate `_fbp` cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

125. Facebook, at a minimum, uses the `fr`, `_fbp`, and `c_user` cookies to link to FIDs and corresponding Facebook profiles.

126. As shown in the above figures, Defendant sent these identifiers with the event data.

127. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant to disclose his personally identifiable information and protected health information; nor did he authorize any assistance with intercepting his communications. Plaintiff was never provided with any written notice that Defendant disclosed its Website users’ protected health information, nor was he provided any means of opting out of such disclosures. Despite this, Defendant knowingly disclosed Plaintiff’s protected health information to Facebook.

128. Although the full scope of Defendant’s illegal data sharing practices is presently unknown, additional evidence demonstrates that Defendant is also sharing its patients’ data with

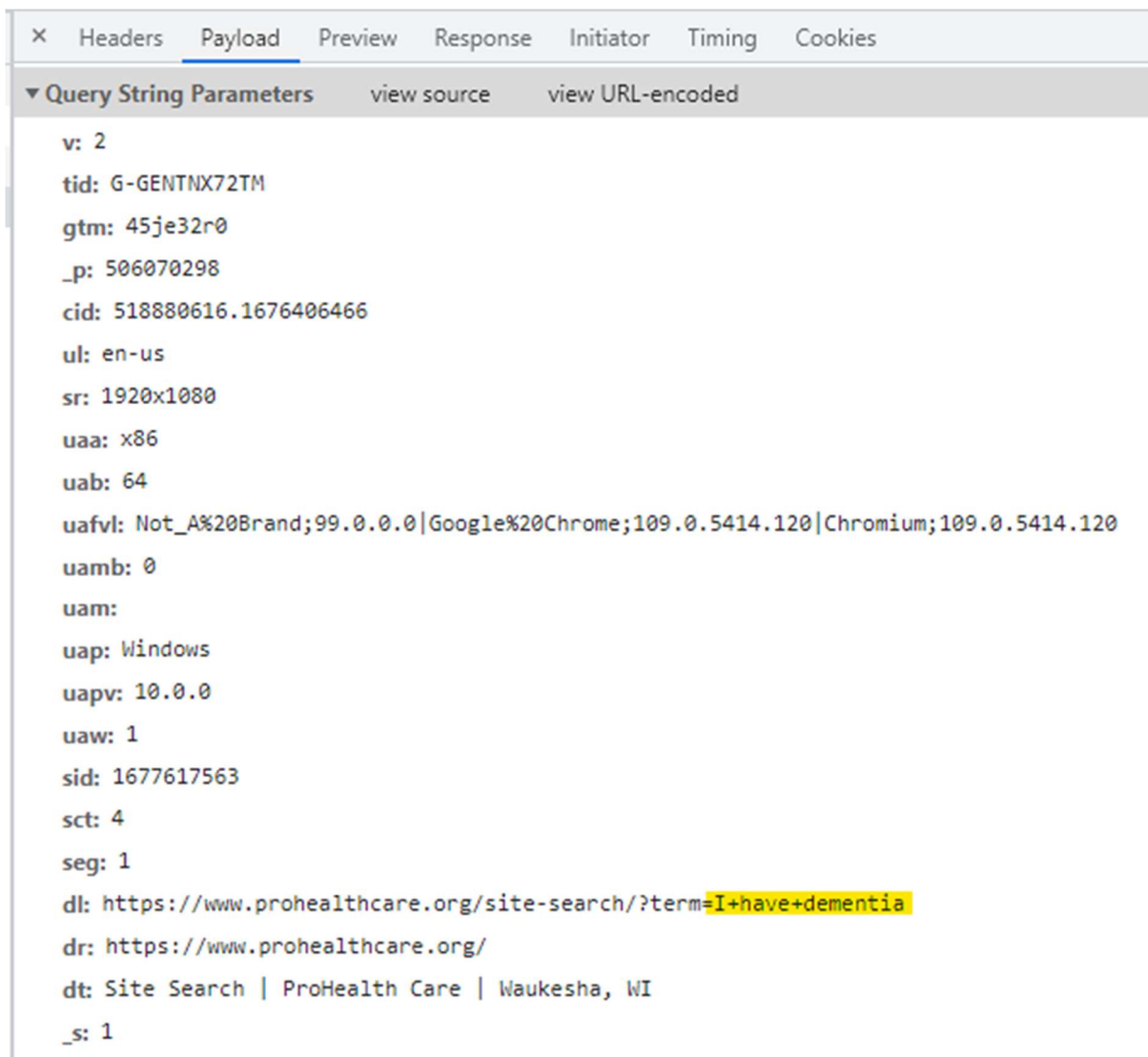
---

<sup>29</sup> Confirmable through developer tools.

<sup>30</sup> *First-Party Cookie*, PCMAG.COM, <https://www.pcmag.com/encyclopedia/term/first-party-cookie> (last visited Jan. 18, 2023). This is confirmable by using developer tools to inspect a website’s cookies and track network activity.

<sup>31</sup> *Third-Party Cookie*, PCMAG.COM, <https://www.pcmag.com/encyclopedia/term/third-party-cookie> (last visited Jan. 18, 2023). This is also confirmable by tracking network activity.

Google via the Google Analytics tools, and the image below indicates that Defendant has failed to enable the “anonymize IP” feature. Resultingly, Google receives a patient’s communications and data alongside their unique IP address, thereby creating an additional and distinct HIPAA violation and breach of confidentiality.



**Figure 14. Images of the data that is sent to Google, which contains the exact phrase and medical condition the user communicated via Defendant’s website.**

129. By law, Plaintiff is entitled to privacy in his protected health information and confidential communications. Defendant deprived Plaintiff and Class Members of their privacy

rights when it: (i) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and Class Members' confidential communications, personally identifiable information, and protected health information to a third party; (ii) disclosed patients' protected information to Facebook – an unauthorized third-party eavesdropper; and (iii) undertook this pattern of conduct without notifying Plaintiff and Class Members and without obtaining their express written consent. Plaintiff did not discover that Defendant disclosed his personally identifiable information and protected health information to Facebook, and assisted Facebook with intercepting is communications, until November 2022.

**D. Defendant's Privacy Policies & Promises**

130. Defendant's privacy policies represent to Plaintiff and Class Members that Defendant will keep Private Information "private and secure" and it will only disclose Private Information under certain circumstances.<sup>32</sup>

131. Defendant publishes several privacy policies that represent to patients and visitors to its Website that ProHealth will keep sensitive information confidential and that it will only disclose PII and PHI provided to it under certain circumstances, *none of which apply here*.

132. Defendant publishes a Health Information Privacy Notice which tells patients that ProHealth is "committed to safeguarding [patients'] private health information and to following state and federal privacy laws."<sup>33</sup>

---

<sup>32</sup> <https://www.prohealthcare.org/patients-families/privacy-policies/> (last visited Jan. 18, 2023).

<sup>33</sup> <https://www.prohealthcare.org/patients-families/privacy-policies/health-information-privacy/> (last visited Jan. 18, 2023).

133. Defendant's Website Privacy Policy assures Plaintiffs and Class Members that "[p]ersonal information provided by you on our website is never given or sold to any other parties."<sup>34</sup>

134. Defendant's Health Information Privacy Notice explains Defendant's legal duties with respect to Private Information and the exceptions for when Defendant can lawfully use and disclose Plaintiffs' and Class Members' Private Information in the following ways:

- To treat you;
- To run our organization;
- To bill for our services;
- To help with public health and public safety issues;
- To conduct research;
- To comply with the law;
- To respond to organ and tissue donations requests;
- To work with a medical examiner or funeral director;
- To address workers' compensation, law enforcement and other government requests;
- To respond to lawsuits and other legal actions.<sup>35</sup>

135. Defendant's privacy policy does **not** permit Defendant to use and disclose Plaintiff's and Class Members' Private Information for marketing purposes. In fact, Defendant's

---

<sup>34</sup> <https://www.prohealthcare.org/patients-families/privacy-policies/website-privacy-policy-and-disclaimer/> (last visited Jan. 18, 2023).

<sup>35</sup> <https://www.prohealthcare.org/patients-families/privacy-policies/health-information-privacy/>



Privacy Notice states: “In the following situations we will not share your information unless you give us written permission:

- Marketing purposes
- Sale of your information [...]”<sup>36</sup>

136. Defendant also acknowledges the following:

We are required by law to maintain the privacy and security of your protected health information.

We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.

We must follow the duties and privacy practices described in this notice and give you a copy of it.

We will not use or share your information other than as described here unless you tell us we may in writing. If you tell us we may, you may change your mind at any time. Let us know in writing if you change your mind.<sup>37</sup>

137. Defendant’s Privacy Notice also states that:

[S]tate and federal law may have more requirements than HIPAA on how we use and disclose your health information. If there are specific, more restrictive requirements, even for some of the purposes listed above, we may not disclose your health information without your written permission as required by such laws.<sup>38</sup>

138. Defendant violated their own privacy policy by unlawfully intercepting and disclosing Plaintiff’s and Class Members’ Private Information to Facebook and third parties without adequately disclosing that Defendant shared Private Information with third parties and without acquiring the specific patients’ consent or authorization to share the Private Information.

---

<sup>36</sup> *Id.*

<sup>37</sup> *Id.*

<sup>38</sup> *Id.*

***E. Federal Warning on Tracking Codes on Healthcare Websites.***

139. Beyond Defendant’s own policies, and those of Meta, the government has issued guidance warning that tracking code like Meta Pixel may come up against federal privacy law when installed on healthcare websites. The statement, titled *Use of Online Tracking Technologies By HIPAA Covered Entities And Business Associates* (the “Bulletin”), was recently issued by the Department of Health and Human Services’ Office for Civil Rights (“OCR”).<sup>39</sup>

140. Healthcare organizations regulated under the Health Insurance Portability and Accountability Act (HIPAA) may use third-party tracking tools, such as Google Analytics or Meta Pixel, in a limited way, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients’ protected health information to these vendors. The Bulletin explains:

Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures.***<sup>40</sup>

141. The bulletin discusses the types of harm that disclosure may cause to the patient:

An impermissible disclosure of an individual’s PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, ***discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual’s PHI.*** Such disclosures can reveal incredibly sensitive information about an individual, ***including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.*** While it has always been true that regulated

---

<sup>39</sup> HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaaonline-tracking/index.html> (last visited Feb. 19, 2023).

<sup>40</sup> Id. (Emphasis added).

entities may not impermissibly disclose PHI to tracking technology vendors, *because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.*<sup>41</sup>

142. Plaintiff and Class members face just the risks about which the government expresses concern. Defendant has passed along Plaintiff's and Class Members' search terms about health conditions for which they seek doctors; their contacting of doctors to make appointments; the names of their doctors; the frequency with which they take steps relating to obtaining healthcare for certain conditions; and where they seek medical treatment. This information is, as described by the OCR in its bulletin, "highly sensitive." The Bulletin goes on to make clear how broad the government's view of protected information is. It explains:

This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, *or any unique identifying code.*<sup>42</sup>

143. Crucially, that paragraph in the government's Bulletin continues:

*All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.*<sup>43</sup>

---

<sup>41</sup> Id. (Emphasis added.)

<sup>42</sup> Id. (Emphasis added.)

<sup>43</sup> Id. (Emphasis added.)

144. This is further evidence that the data that Defendant chose to share is protected Personal Information. The sharing of that information was a violation of Class Members' rights.

***F. Defendant's Violation of HIPAA***

145. Defendant's disclosure of Plaintiff's and Class Members' Private Information to entities like Facebook also violated HIPAA. HIPAA provided Plaintiff and Class members with another reason to believe that the information they communicated to Defendant through its Website would be protected, rather than shared with third-parties for marketing purposes.

146. HIPAA's Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

147. HIPAA prohibits health care providers from "us[ing] or disclos[ing] 'protected health information' except as permitted or required by" the HIPAA Privacy Rule. 45 C.F.R. § 164.502.

148. "A covered entity may determine that health information is not individually identifiable health information only if" either "a person with appropriate knowledge of and experience with generally accepted statistical and scientific methods for rendering information not individually identifiable: a) applying such principles" determines that the risk is "very small" that the information could be used alone, or in combination with other information, to identify individuals, and documents the methods that justifies such a determination, or identifiers are

removed that include: Internet Protocol (IP) address numbers; account numbers; URLs, device identifiers, and “any other unique identifying number, characteristic or code,” except codes assigned by the healthcare organization to allow itself to reidentify information from which it has removed identifying information.

149. Even the fact that an individual is receiving a medical service, i.e., is a patient of a particular entity, can be Protected Health Information. The Department of Health and Human Services has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook because it is not related to health data:

If such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.<sup>44</sup>

150. Consistent with this restriction, the HHS has issued marketing guidance that provides that: With limited exceptions, the [Privacy] Rule requires an individual’s written authorization before a use or disclosure of his or her protected health information can be made for marketing. ... Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party’s own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.<sup>45</sup>

---

<sup>44</sup> HHS.gov, GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE, <https://www.hhs.gov/hipaa/forprofessionals/privacy/special-topics/de-identification/index.html> (last visited Feb. 19, 2023).

<sup>45</sup> HHS.gov, MARKETING, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html> (last visited Feb. 20, 2023).

151. Here, Defendant provided patient information to third parties in violation of this rule.

152. Commenting on a June 2022 report discussing the use of the Meta Pixel by hospitals and medical centers, David Holtzman, a health privacy consultant and a former senior privacy adviser in HHS OCR, which enforces HIPAA, stated, “I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it...It is quite likely a HIPAA violation.”<sup>46</sup>

153. Defendant’s placing of the third-party tracking code on its Website is a violation of Class Members’ privacy rights under federal law. While Plaintiff does not bring a claim under HIPAA itself, this violation evidences Defendant’s wrongdoing as relevant to other claims.

***G. Plaintiff’s & Class Members’ Private Information Has Financial Value.***

154. Plaintiff’s private data has economic value. Indeed, Meta’s, Google’s and others’ practices of using such information to package groups of people as “Lookalike Audiences” and similar groups and selling those packages to advertising clients demonstrates the financial worth of that data.

155. Data harvesting is the fastest growing industry in the nation. As software, data mining, and targeting technologies have advanced, the revenue from digital ads and the consequent value of the data used to target them have risen rapidly.

156. Consumer data is so valuable that some have proclaimed that data is the new oil. Between 2016 and 2018, the value of information mined from Americans increased by 85% for

---

<sup>46</sup> HHS.gov, Advisory Board, 'DEEPLY TROUBLED': SECURITY EXPERTS WORRY ABOUT FACEBOOK TRACKERS ON HOSPITAL SITES, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html> (last visited Feb. 20, 2023).

Facebook and 40% for Google. Overall, the value internet companies derive from Americans' personal data increased almost 54%. Conservative estimates suggest that in 2018, Internet companies earned \$202 per American user. In 2022, that value is expected to be \$200 billion industry wide, or \$434 per user, also a conservative estimate.

157. As to health data specifically, as detailed in an article in Canada's National Post:

As part of the multibillion-dollar worldwide data brokerage industry, health data is one of the most sought-after commodities. De-identified data can be re-identified (citing <https://www.nature.com/articles/s41467-019-10933-3/> ) and brazen decisions to release records with identifiable information (citing [https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200?mod=hp\\_list\\_pos3](https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200?mod=hp_list_pos3) ) are becoming commonplace).<sup>47</sup>

158. Further demonstrating the financial value of Class Members' medical data, CNBC has reported that hospital executives have received a growing number of bids for user data:

Hospitals, many of which are increasingly in dire financial straits, are weighing a lucrative new opportunity: selling patient health information to tech companies. Aaron Miri is chief information officer at Dell Medical School and University of Texas Health in Austin, so he gets plenty of tech start-ups approaching him to pitch deals and partnerships. Five years ago, he'd get about one pitch per quarter. But these days, with huge data-driven players like Amazon and Google making incursions into the health space, and venture money flooding into Silicon Valley start-ups aiming to bring machine learning to health care, the cadence is far more frequent. "It's all the time," he said via phone. "Often, once a day or more."

\* \* \*

[H]ealth systems administrators say [the data] could also be used in unintended or harmful ways, like being cross-referenced with other data to identify individuals at higher risk of diseases and then raise their health premiums, or to target advertising to individuals.<sup>48</sup>

---

<sup>47</sup> National Post, IRIS KULBATSKI: THE DANGERS OF ELECTRONIC HEALTH RECORDS, February 26, 2020, <https://nationalpost.com/opinion/iris-kulbatki-the-dangers-of-electronic-health-records> (last visited Feb. 20, 2023).

<sup>48</sup> CNBC, HOSPITAL EXECS SAY THEY ARE GETTING FLOODED WITH REQUESTS FOR YOUR HEALTH DATA, <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited Feb. 2023).

159. The CNBC article also explained:

De-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers. Just one company alone, IQVIA, said on its website that it has access to more than 600 million patient records globally that are nonidentified, much of which it accesses through provider organizations. The buyers, which include pharma marketers, will often use it for things like clinical trial recruiting. But hospital execs worry that this data may be used in unintended ways, and not always in the patient's best interest.

\* \* \*

160. Tech companies are also under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own needs. For instance, the health data Google collects could eventually help it micro-target advertisements to people with particular health conditions. Policymakers are proactively calling for a revision and potential upgrade of the health privacy rules known as HIPAA, out of concern for what might happen as tech companies continue to march into the medical sector.<sup>49</sup>

161. Time Magazine similarly, in an article titled, *How your Medical Data Fuels A Hidden Multi-Billion Dollar Industry*, referenced the "growth of the big health data bazaar," in which patients' health information is sold. It reported that:

[T]he secondary market in information unrelated to a patient's direct treatment poses growing risks, privacy experts say. That's because clues in anonymized patient dossiers make it possible for outsiders to determine your identity, especially as computing power advances in the future.<sup>50</sup>

---

<sup>49</sup> *Id.*

<sup>50</sup> Time, HOW YOUR MEDICAL DATA FUELS A HIDDEN MULTI-BILLION DOLLAR INDUSTRY, <https://time.com/4588104/medical-data-industry/> (last visited Feb. 20, 2023).



162. ProHealth gave away Plaintiff's and Class Members' communications and transactions on its Website without permission. The unauthorized access to Plaintiff's and Class Members' private and Personal Information has diminished the value of that information, resulting in harm to Defendant's Website users.

#### ***H. Defendant Violated Industry Standards***

163. A medical provider's duty of confidentiality is embedded in the physician-patient and hospital-patient relationship, it is a cardinal rule.

164. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

165. AMA Code of Ethics Opinion 3.1.1 provides:

Protecting information gathered in association with the care of the patient is a core value in health care... Patient privacy encompasses a number of aspects, including, ... personal data (informational privacy)[.]

166. AMA Code of Medical Ethics Opinion 3.2.4 provides:

Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

167. AMA Code of Medical Ethics Opinion 3.3.2 provides:

Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information

electronically...must: (c) Release patient information only in keeping ethics guidelines for confidentiality.<sup>51</sup>

***I. Plaintiff's & Class Members' Expectation of Privacy***

168. Plaintiff and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

169. Indeed, at all times when Plaintiff and Class Members provided their PII and PHI to Defendant, they each had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

***J. IP Addresses are Personally Identifiable Information***

170. In addition to patient status, medical conditions, treatment, specific providers, appointment information, and patient's unique and persistent Facebook ID, Defendant improperly disclosed patients' computer IP addresses to Facebook through the use of the Pixel.

171. An IP address is a number that identifies the address of a device connected to the Internet.

172. IP addresses are used to identify and route communications on the Internet.

173. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

174. Facebook tracks every IP address ever associated with a Facebook user.

175. Google also tracks IP addresses associated with Internet users.

---

<sup>51</sup> <https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf> (last visited December 20, 2022).

176. Facebook, Google, and other third-party marketing companies track IP addresses for use of tracking and targeting individual homes and their occupants with advertising by using IP addresses.

177. Under HIPAA, an IP address is considered personally identifiable information:

178. HIPAA defines personally identifiable information to include “any unique identifying number, characteristic or code” and specifically lists the example of IP addresses. See 45 C.F.R. § 164.514 (2).

179. HIPAA further declares information as personally identifiable where the covered entity has “actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.” 45 C.F.R. § 164.514(2)(ii); See also, 45 C.F.R. § 164.514(b)(2)(i)(O).

180. Consequently, Defendant’s disclosure of patients’ IP addresses violated HIPAA and industry privacy standards.

***K. Defendant was Enriched & Benefitted from the Use of The Pixel & Unauthorized Disclosures***

181. The sole purpose of the use of the Facebook Pixel on Defendant’s Website was marketing and profits.

182. In exchange for disclosing the personally identifiable information of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on Facebook.

183. Upon information and belief, Defendant was advertising its services on Facebook, and the Pixel was used to “help [Defendant] understand the success of [its] advertisement efforts on Facebook.”

184. Retargeting is a form of online marketing that targets users with ads based on their previous Internet communications and interactions.

185. Upon information and belief, Defendant re-targeted patients and potential patients to get more patients to use its services.

186. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

***L. Representative Plaintiff John Doe's Experiences***

187. As a condition of receiving Defendant's services, Plaintiff Doe disclosed his Private Information to Defendant on numerous occasions, and most recently in December 2022.

188. Plaintiff Doe accessed Defendant's Website on his phone and computer to receive healthcare services from Defendant and at Defendant's direction.

189. Plaintiff Doe scheduled doctor's appointments for himself via the Defendant's Website.

190. Plaintiff Doe has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

191. Plaintiff Doe reasonably expected that his communications with Defendant via the Website were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

192. Plaintiff Doe provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

193. As described herein, Defendant worked along with Facebook to intercept Plaintiff Doe's communications, including those that contained Private and confidential information.

194. Defendant willfully facilitated these interceptions without Plaintiff Doe's knowledge, consent, or express written authorization.

195. Defendant transmitted to Facebook Plaintiff Doe's Facebook ID, computer IP address, and information such as appointment type, physician selected, button/menu selections, and/or content typed into free text boxes.

196. By doing so without Plaintiff Doe's consent, Defendant breached Plaintiff Doe's privacy and unlawfully disclosed his private information.

197. Defendant did not inform Plaintiff Doe that it had shared his Private Information with Facebook.

198. Plaintiff Doe is diagnosed with a specific medical condition and submitted information to Defendant's Website about scheduling medical appointments for his condition.

199. Plaintiff Doe suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to his Private Information.

200. Plaintiff Doe has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

#### **IV. TOLLING**

201. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that Plaintiff's PII and PHI was intercepted and unlawfully disclosed because Defendant kept this information secret.

## **V. CLASS ACTION ALLEGATIONS**

202. Plaintiff Doe brings this action on behalf of himself and on behalf of all other persons similarly situated (the “Class”) pursuant to Rule 23(b)(2), 23(b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure.

203. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Pixel on Defendant’s Website.

204. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

205. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

206. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The Nationwide Class members are so numerous that joinder of all members is impracticable. Upon information and belief, there are over one million individuals whose PII and PHI may have been improperly accessed by Facebook, and the Class is identifiable within Defendant’s records.

207. **Commonality & Predominance, Fed. R. Civ. P. 23(a)(2) and (b)(3):** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;
- b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;

- c. Whether Defendant violated its privacy policy by disclosing the PII and PHI of Plaintiff and Class Members to Facebook, Meta, and/or additional third parties.
- d. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI would be disclosed to third parties;
- e. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;
- f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient PHI and PII;
- g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;
- h. Whether Defendant violated the consumer protection statutes invoked herein;
- i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- j. Whether Defendant knowingly made false representations as to its data security and/or privacy policy practices;
- k. Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy policy practices and
- l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendant's disclosure of their PII and PHI.

208. **Typicality, Fed. R. Civ. P. 23(a)(3)**: Plaintiff's claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

209. **Adequacy, Fed. R. Civ. P. 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

210. **Superiority and Manageability, Fed. R. Civ. P. 23(b)(3):** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

211. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class



Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

212. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

213. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

214. **Ascertainability & Notice:** Membership in the Class can be determined by objective records maintained by Defendant and adequate notice can be given to Class Members directly using information maintained in Defendant's records.

215. **Class-wide Injunctive Relief, Fed. R. Civ. P. 23(b)(2):** Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to

act unlawfully as set forth in this Complaint as Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

216. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information;
- b. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information with respect to Defendant's privacy policy;
- c. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- e. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;
- f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties and
- g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.<sup>52</sup>

---

<sup>52</sup> Plaintiff reserves the right to amend or modify the Class definition as this case progresses.

**COUNT I**  
**INVASION OF PRIVACY**  
**(On Behalf of Plaintiff & the Class)**

217. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

218. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

219. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website and the communications platforms and services therein.

220. Plaintiff and Class Members communicated sensitive and protected medical information and individually identifiable information that they intended for only Defendant to receive and that they understood Defendant would keep private.

221. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiffs and Class Members is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion.

222. Plaintiff's and Class Members had a reasonable expectation of privacy given Defendant's representations, HIPAA Notice of Privacy Practices and Privacy Policy.

223. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential. Defendant's disclosure of private medical information coupled with individually identifying information is highly offensive to the reasonable person.

224. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

225. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

226. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiffs' and Class Members' privacy.

227. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant's from engaging in such conduct in the future.

228. Plaintiff also seeks such other relief as the Court may deem just and proper.

**COUNT II**  
**UNJUST ENRICHMENT**  
**(On behalf of Plaintiff & the Class)**

229. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

230. Defendant benefitted from Plaintiff and Class Members and unjustly retained those benefits at their expense.

231. Plaintiff and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation. Defendant consciously collected and used this information

for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

232. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

233. The benefits that Defendant derived from Plaintiff and Class Members was not offered by Plaintiff and Class Member gratuitously and rightly belongs to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles in Wisconsin and every other state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

234. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

**COUNT III**  
**BREACH OF CONFIDENCE**  
**(On behalf of Plaintiff & the Class)**

235. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

236. Medical providers have a duty to their patients to keep non-public medical information completely confidential.

237. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website, which were further buttressed by Defendant's express promises in its privacy policy.

238. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Pixel and CAPI to disclose and transmit to third parties Plaintiff's and Class Members' communications with Defendant, including Private Information and the contents of such information.

239. These disclosures were made without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged.

240. The third-party recipients included, but were not limited to, Facebook.

241. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

242. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class Members were damaged by Defendant's breach in that:

- a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;
- b. Plaintiff and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
- d. General damages for invasion of their rights in an amount to be determined by a jury;
- e. Nominal damages for each independent violation;
- f. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;

- g. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- h. Defendant's actions diminished the value of Plaintiff's and Class Members' Personal Information; and
- i. Defendant's actions violated the property rights Plaintiff and Class members have in their Personal Information.

**COUNT IV**  
**VIOLATION OF CONFIDENTIALITY OF PATIENT HEALTH CARE RECORDS**  
**Wis. Stat. § 146.81, *et seq.***  
**(On Behalf of Plaintiff & the Class)**

243. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

244. Under Wisconsin law all patient health care records must remain confidential and patient health care records may only be released to a person upon the informed consent of the patient, or as authorized by the patient.

245. Defendant disclosed the private and protected medical information of Plaintiff and Class Members to unauthorized third parties without their knowledge, consent, or authorization.

246. ProHealth is a healthcare provider as defined by Wis. Stat. Ann. § 146.816(1).

247. Plaintiff and Class Members are patients, and, as a health care provider, Defendant had and has an ongoing obligation not to disclose their Private Information.

248. The Private information disclosed by Defendant is protected health information as defined by Wis. Stat. Ann. § 146.816(f).

249. Defendant violated Wis. Stat. § 146.81, *et seq.* through its willful and knowing failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the Class Members. Defendant's conduct with respect to the disclosure of its patients' confidential

Private Information was willful and knowing because Defendant configured and implemented the digital platforms and tracking software that gave rise to sharing patients' PII and PHI with third parties.

250. Plaintiff and Class Members were injured as a result of ProHealth's violation of the confidentiality of patient health care law.

251. As a result of its intentional and willful disclosure of Plaintiff and Class Members' Private Information, Defendant is liable for actual damages, additional damages of at least \$25,000 if the violation was willful or \$1,000 otherwise, and the costs and attorneys' fees incurred as a result of the violation. Wis. Sta. Ann. § 146.84.

**COUNT V**  
**VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")**  
**18 U.S.C. § 2511(1) *et seq.***  
**UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE**  
**(On Behalf of Plaintiff & the Class)**

252. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

253. The ECPA protects both sending and receipt of communications.

254. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

255. The transmissions of Plaintiff's PII and PHI to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

256. **Electronic Communications.** The transmission of PII and PHI between Plaintiff and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,...data, [and] intelligence of [some] nature transmitted in



whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo optical system that affects interstate commerce” and are therefore “electronic communications” within the meaning of 18 U.S.C. § 2510(2).

257. **Content.** The ECPA defines content, when used with respect to electronic communications, to “include [] *any* information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8).

258. **Interception.** The ECPA defines the interception as the “acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device” and “contents...include any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(4), (8).

259. **Electronic, Mechanical or Other Device.** The ECPA defines “electronic, mechanical, or other device” as “any device...which can be used to intercept a[n]...electronic communication[.]” 18 U.S.C. § 2510(5). The following constitute “devices” within the meaning of 18 U.S.C. § 2510(5):

- a. Plaintiff’s and Class Members’ browsers;
- b. Plaintiff’s and Class Members’ computing devices;
- c. Defendant’s web-servers;
- d. Defendant’s Website; and
- e. The Pixel code deployed by Defendant to effectuate the sending and acquisition of patient communications.

260. By utilizing and embedding the Pixel on its Website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic

communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

261. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the Pixel, which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' PII to Facebook.

262. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiff's and Class Members' regarding PII and PHI, treatment, medication, and scheduling.

263. By intentionally disclosing or endeavoring to disclose the electronic communications of the Plaintiff and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

264. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

265. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

266. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

267. Defendant was not acting under color of law to intercept Plaintiff and the Class Member's wire or electronic communication.

268. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's privacy via the Pixel tracking code.

269. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

270. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendant's Website, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions, including as described above the following: (i) a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person; and (ii) violation of Wis. Stat. § 146.81, *et seq.*

**COUNT VI**  
**VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT**  
**UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE**  
**18 U.S. Code § 2511(3)(a)**  
**(On Behalf of Plaintiff & the Class)**

271. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

272. The ECPA statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission

on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.” 18 U.S.C. § 2511(3)(a).

273. **Electronic Communication Service.** An “electronic communication service” is defined as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15).

274. Defendant’s Website is an electronic communication service which provides to users thereof the ability to send or receive electronic communications. In the absence of Defendant’s website, internet users could not send or receive communications regarding Plaintiff’s and Class Members’ PII and PHI.

275. **Intentional Divulgence.** Defendant intentionally designed the Pixel tracking and was or should have been aware that, if misconfigured, it could divulge Plaintiff’s and Class Members’ PII and PHI.

276. **While in Transmission.** Upon information and belief, Defendant’s divulgence of the contents of Plaintiff’s and Class Members’ communications was contemporaneous with their exchange with Defendant’s Website, to which they directed their communications.

277. Defendant divulged the contents of Plaintiff’s and Class Members’ electronic communications without authorization. Defendant divulged the contents of Plaintiff’s and Class Members’ communications to Facebook without Plaintiff’s and Class Members’ consent and/or authorization.

278. **Exceptions do not apply.** In addition to the exception for communications directly to an electronic communications service (“ECS”)<sup>53</sup> or an agent of an ECS, the ECPA states that

---

<sup>53</sup> An ECS is “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15).

“[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication.”

- a. “as otherwise authorized in section 2511(2)(a) or 2517 of this title;”
- b. “with the lawful consent of the originator or any addressee or intended recipient of such communication;”
- c. “to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;” or
- d. “which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.”

U.S.C. § 2511(3)(b).

279. Section 2511(2)(a)(i) provides:

It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

280. Defendant’s divulgence of the contents of Plaintiff’s and Class Members’ communications on Defendant’s website to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendant’s service; nor (2) necessary to the protection of the rights or property of Defendant.

281. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

282. Defendant's divulgence of the contents of user communications on Defendant's Website through the Pixel code was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiff and Class Members were exchanging information.

283. Moreover, Defendant divulged the contents of Plaintiff's and Class Members' communications through the Pixel code to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

284. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

285. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

**COUNT VII**  
**VIOLATION OF**  
**TITLE II OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT**  
**18 U.S.C. § 2702, *et seq.***  
**(STORED COMMUNICATIONS ACT)**  
**(On Behalf of Plaintiff & the Class)**

286. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

287. The ECPA further provides that “a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” 18 U.S.C. § 2702(a)(1).

288. **Electronic Communication Service.** ECPA defines “electronic communications service” as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15).

289. Defendant intentionally procures and embeds various Plaintiff’s PII and PHI through the Pixel used on Defendant’s Website, which qualifies as an Electronic Communication Service.

290. **Electronic Storage.** ECPA defines “electronic storage” as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof” and “any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17).

291. Defendant stores the content of Plaintiff’s and Class Members’ communications on Defendant’s Website and files associated with it.

292. When Plaintiff or Class Members make a Website communication, the content of that communication is immediately placed into storage.

293. Defendant knowingly divulges the contents of Plaintiff’s and Class Members’ communications through the Pixel.

294. **Exceptions Do Not Apply.** Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider “may divulge the contents of a communication—”

- a. “to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.”
- b. “as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;”
- c. “with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;”
- d. “to a person employed or authorized or whose facilities are used to forward such communication to its destination;”
- e. “as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;”
- f. “to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A.”
- g. “to a law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;”
- h. “to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency”; or
- i. “to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523.”

295. Defendant did not divulge the contents of Plaintiff’s and Class Members’ communications to “addressees,” “intended recipients,” or “agents” of any such addressees or intended recipients of Plaintiff and Class Members.

296. Section 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.



297. Section 2511(2)(a)(i) provides:

It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

298. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications on Defendant's Website to Facebook or other third parties was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of the Defendant's services; nor (2) necessary to the protection of the rights or property of Defendant.

299. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

300. Defendant's divulgence of the contents of user communications on Defendant's Website was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiff and Class Members were exchanging information.

301. Moreover, Defendant divulged the contents of Plaintiff and Class Members' communications through the Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

302. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

303. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

**COUNT VIII**  
**VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (CFAA)**  
**18 U.S.C. § 1030, *et seq.***  
**(On Behalf of Plaintiff & the Class)**

304. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

305. Plaintiff's and the Class Members' computers and mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

306. Defendant exceeded, and continues to exceed, authorized access to the Plaintiff's and the Class Members' protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

307. Defendant's conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiff's and the Class Members' private and personally identifiable data and content – including the Website visitor's electronic communications with the Website, including their mouse movements, clicks, keystrokes (such as text being entered into an

information field or text box), URLs of web pages visited, and/or other electronic communications in real-time (“Website Communications”) which were never intended for public consumption.

308. Defendant’s conduct also constitutes “a threat to public health or safety” under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally identifiable data and content of Plaintiff and the Class Members’ Website Communications being made available to Defendant, Facebook, and/or other third parties without adequate legal privacy protections.

309. Accordingly, Plaintiff and the Class Members are entitled to “maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.” 18 U.S.C. § 1030(g).

### **PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff John Doe respectfully prays for judgment as follows:

- For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and Plaintiff’s counsel as Class Counsel;
- For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff’s and Class Members’ Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI disclosed to third parties;
- For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant’s wrongful conduct;

- For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- For an award of punitive damages, as allowable by law;
- For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- Pre- and post-judgment interest on any amounts awarded and
- All such other and further relief as this court may deem equitable and just.

### **DEMAND FOR JURY TRIAL**

Plaintiff hereby demands that this matter be tried before a jury.

Date: March 3, 2023

Respectfully submitted,

**HANSEN REYNOLDS LLC**

/s/ Timothy M. Hansen  
 Timothy M. Hansen (SBN 1044430)  
 Michael C. Lueder (SBN 1039954)  
 301 N. Broadway, Suite 400  
 Milwaukee, Wisconsin 53202  
 (414) 455-7676 (phone)  
 (414) 273-8476 (fax)  
 thansen@hansenreynolds.com  
 mlueder@hansenreynolds.com

**ALMEIDA LAW GROUP LLC**

David S. Almeida (SBN 1086050)  
 849 W. Webster Avenue  
 Chicago, Illinois 60614  
 (312) 576-3024 (phone)  
 david@almeidalawgroup.com

**MILBERG COLEMAN BRYSON  
PHILLIPS GROSSMAN, PLLC**

Gary M. Klinger  
227 Monroe Street, Suite 2100  
Chicago, IL 60606  
(866) 252-0878 (phone)  
gklinger@milberg.com

*Attorneys for Plaintiff & the Putative Class*